

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

<hr/>	x	
In re SONY BMG CD TECHNOLOGIES	:	Civil Action No. 1:05-cv-09575-NRB
LITIGATION	:	
<hr/>	:	<u>CLASS ACTION</u>
	:	
This Document Relates To:	:	REPLY DECLARATION OF J. ALEX
	:	HALDERMAN IN SUPPORT OF RICCIUTI
	:	CLASS REPRESENTATIVES' MOTION
ALL ACTIONS.	:	FOR AN AWARD OF ATTORNEYS' FEES
<hr/>	x	AND REIMBURSEMENT OF EXPENSES
		[CORRECTED]

I, J. Alex Halderman, hereby declare as follows:

1. I am a Ph.D. candidate in computer science at Princeton University. My research interests include computer security, digital rights management, information privacy, and the interplay between technology and public policy. My advisor is Professor Edward Felten. Along with Professor Felten, I regularly post on the Freedom to Tinker blog, located at: [www.freedom-to-tinker.com](http://www.freedom-to-tinker.com). I have authored, co-authored or assisted in all of the postings on the blog relating to MediaMax DRM software. I have personal knowledge of the matters stated herein, and if called upon, I could and would competently testify thereto.

2. From June 2003, to the present I have been a research assistant at the Princeton University Secure Internet Programming Laboratory. As part of an activate research agenda, I have engaged in projects including denial-of-service defenses for network servers, novel methods for managing user passwords, cryptographic privacy-management techniques for recording devices such as camera phones, and client puzzle approaches to the Sybil attack problem in distributed systems.

3. I have also performed analysis and security evaluation of digital rights management ("DRM") for audio CDs that has received world-wide media attention.

4. My publications are available online at <http://www.cs.princeton.edu/~jhalderm/papers/>. They include the following:

- (a) Lessons from the Sony CD DRM Episode, with Professor Edward Felten;
- (b) Digital Rights Management, Spyware, and Security;
- (c) A Convenient Method for Securely Managing Passwords;
- (d) Privacy Management for Portable Recording Devices;
- (e) New Client Outsourcing Techniques for DoS Protection;
- (f) Analysis of the MediaMax CD3 Copy-Prevention System;

- (g) Early Experiences with a 3D Model Search Engine;
  - (h) A Search Engine for 3D Models; and
  - (i) Evaluating New Copy-Prevention Techniques for Audio CDs.
5. I have received the following awards for my work:
- (a) National Science Foundation Graduate Research Fellowship (2004);
  - (b) Princeton Computer Science Department graduate study award (2003);
  - (c) Princeton Computer Science Department Senior Award (2003);
  - (d) Accenture Prize in Computer Science (2002);
  - (e) Martin A. Dale Summer Award (2000); and
  - (f) Election to honorific societies, including Phi Beta Kappa and Sigma Xi.

**I. Mr. Jacobson Misstates My Role in the MediaMax 5.0 ACL Problem**

6. Mr. Jacobson's declaration states that over the Thanksgiving holiday, the Freedom to Tinker website indicated a "theoretical" privilege escalation security problem and that EFF subsequently brought that problem to Sony BMG's attention on November 30, 2006. Declaration of Jeffrey S. Jacobson, Esq., in Opposition to the "EFF Group's" Motion for the Award of Attorneys' fees ("Jacobson Decl."), ¶19. This incorrectly conflates two security problems which are distinct.

7. The privilege escalation security problem, also called an ACL problem, was discovered by Jesse Burns and Alex Stamos of iSEC Security Partners and is different from the problems that were discussed by Professor Felten and me in late November. iSEC discovered that the MediaMax installer sets file permissions that allow any user to modify its code directory and the files and programs in it. As Burns and Stamos realized, the lax permissions allow a non-privileged user to replace the executable code in the MediaMax player files with malicious code. The next time a user plays a MediaMax-protected CD, the attack code will be executed with that user's security privileges. The MediaMax player requires Power User or Administrator privileges to run, so it is

likely that the attacker's code will run with almost complete control of the system. Normally, this problem could be fixed by manually correcting the errant permissions. However, MediaMax aggressively updates the installed player code each time the software on a protected disc autoruns or is launched manually. As part of this update, the permissions on the installation directory are reset to the insecure state.

8. I first learned about the ACL problem from a document provided by EFF and iSEC on December 6, 2006, the day that EFF and Sony BMG made their joint public announcement about the problem and the initial patch to solve it. Later that day Professor Felten and I verified the existence of the problem as described in the iSEC report.

9. Professor Felten and I did discover that the initial patch released by Sony-BMG on December 6, 2006 in response to the iSEC report was capable of triggering precisely the kind of attack it was supposed to prevent. In the process of updating MediaMax, the patch checked the version of MediaMax.dll by invoking executable code within that file. If this file was already modified by an attacker, the process of applying the security patch would execute the attack code. Prior versions of the MediaMax uninstaller had the same vulnerability, though both the uninstaller and the patch have since been replaced with versions that to my knowledge do not suffer from this problem.

## **II. My Investigation of MediaMax DRM Revealed Many Other Problems, and Confirmed the Seriousness of the MediaMax 5.0 ACL Problem**

10. Mr. Jacobson asserts that "word" of the ACL problem was posted on the Freedom to Tinker website on November 30, 2005. Jacobson Decl., ¶29. This is not true. Professor Felten and I could not have written about the ACL problem on that date, because we did not know about the problem until we learned about iSEC's discovery on December 6, 2006. The only posting on the website on November 30, 2005 was one noting that Sony BMG had been alerted to the XCP rootkit

problem in early October, 2005 and had ignored the alert. Attached hereto as Exhibit 1 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=937>.<sup>1</sup>

11. While I discovered some problems with the MediaMax DRM software in November, 2005, I did not discover or publish the ACL problem, which was discovered by iSEC Partners working with EFF. Specifically:

(a) On November 12, 2006, I published a report that MediaMax software installed prior to user consent. Attached hereto as Exhibit 2 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=925>.

(b) On November 17, I published a report that the uninstaller that Sony BMG created for MediaMax software, in order to allow people to remove the software that had been installed without their consent, itself caused a critical security problem on every computer on which it was used. Professor Felten and I worked with Sony BMG to fix this problem and issue an updated uninstaller. Attached hereto as Exhibit 3 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=931>.

(c) On November 22, 2005, immediately after EFF filed its suit, Professor Felten published a report noting that EFF's lawsuit correctly focused on MediaMax, unlike the other litigation. The post stated: "Emphasizing MediaMax seems like a smart move – while Sony has issued an apology of sorts for XCP and has recalled XCP discs, the company is still stonewalling on MediaMax, even though MediaMax raises issues almost as serious as XCP." Attached hereto as Exhibit 4 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=934>. Note that this posting was prior to the discovery of the ACL problem by iSEC

---

<sup>1</sup> The complete text of all postings on Freedom to Tinker is available on the website archives and linked from our front page: <http://www.freedom-to-tinker.com>.

working with EFF. This additional problem made the risk to MediaMax purchasers even more acute.

(d) On December 7, 2005, after the public announcement of the ACL flaw found by iSEC Partners, I helped Professor Felten write a report about it on Freedom to Tinker website, including our discovery that the patch created by Sony BMG was defective and required yet another patch to fix. Attached hereto as Exhibit 5 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=942>

(e) On December 8, 2005, I again assisted Professor Felten in posting about the security flaw discovered by iSEC, in a post entitled: "Not Just Another Buggy Program." Attached hereto as Exhibit 6 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=944>. The post again emphasizes the seriousness of the security flaw found by iSEC and EFF and ends: "Sony is still shipping CDs containing this dangerous software."

12. In a posting on the website on November 10, 2005, Professor Felten explained why we had come to the conclusion that both the XCP and MediaMax software were spyware. Attached hereto as Exhibit 7 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=923>. The post states:

"In all the discussion of the SonyBMG software, I've been avoiding the S-word. But now it's clear that this software crosses the line. It's spyware.

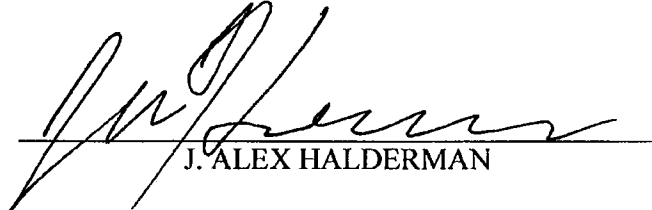
Let's review the evidence:

- The software comes with a EULA which, at the very least, misleads users about what the software does.
- The software interferes with the efforts of ordinary users and programs, including virus checkers and other security software, to identify it.
- Without telling the user or obtaining consent, the software sends information to the vendor about the user's activities.

- No uninstaller is provided with the software, or even on the vendor's website, despite indications to the contrary in the EULA.
- The vendor has an uninstaller but refuses to make it available except to individual users who jump through a long series of hoops.
- The vendor makes misleading statements to the press about the software."

13. In my first post explaining the XCP software on November 2, 2005, I explained why and how it acts like a rootkit, and how the risks it creates for users are the same as those created by many other rootkits. Attached hereto as Exhibit 8 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=920>.

I declare under penalty of perjury under the laws of the State of New York that the foregoing is true and correct. Executed this 11th day of May, 2006, at Princeton, New Jersey.



J. ALEX HALDERMAN

C:\DOCUME~1\User\LOCALS~1\Temp\MetaSave\DEC00030829.doc

# EXHIBIT 1



# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [MediaMax Permanently Installs and Runs Unwanted Software, Even If User Declines EULA](#)  
[The DMCA Should Not Protect Spyware](#) »

## Sony, First4 Knew About Rootkit Issue in Advance

Wednesday November 30, 2005 by Ed Felten

Security vendor F-Secure contacted SonyBMG and First4Internet about the companies' rootkit software on October 4 — about four weeks before the issue became public — according to a Business Week [story](#) by Steve Hamm.

Here's the key part of the article's chronology:

Nevertheless, Sony BMG asked First4Internet to investigate. Both Sony BMG and F-Secure say that it was on Oct. 17 that F-Secure first spelled out the full scope of the problem to Sony. The security company's report on the matter, sent that day to First4Internet and Sony BMG, confirmed there was a rootkit in XCP and warned that it made it possible for hackers to hide viruses and protect them from antivirus software products. F-Secure referred to XCP as a "major security risk," according to a copy of the e-mail supplied to BusinessWeek Online by F-Secure.

Sony BMG says it asked the two software companies to investigate and find a solution to the problem. "From the moment our people learned that F-Secure had identified a potential problem we contacted our vendor and in no uncertain terms told them you have to get with F-Secure and find out what needs to be done about it," says Daniel Mandil, Sony BMG's general counsel.

BOGGED DOWN. What happened next is in dispute. F-Secure had a conference call with executives of First4Internet on Oct. 20. It says First4Internet argued that there was no real problem because only a few people knew of the vulnerability XCP created, and said an update of the XCP software, due out early next year, would fix the problem on all future CDs.

At first glance, this looks like a standard story about disclosure of a security vulnerability: vendor ships insecure product; researchers report flaw privately; vendor drags feet; researchers report flaw publicly; problem fixed right away. The story features the classic vendor error of seeing insecurity as a public relations problem rather than a customer safety issue: "there was no real problem because only a few people knew of the vulnerability".

But if we read this as just another vulnerability disclosure, we're missing an important part of the story. In the usual case, the security vulnerability exists by mistake — the vendor doesn't know the vulnerability exists until somebody points it out. Here, the rootkit-like functionality was not a mistake but a *deliberate design decision* by the vendor.

Which suggests the question of what exactly F-Secure was disclosing to Sony and First4Internet, or more precisely what it was disclosing that they didn't already know. They must have known about the rootkit already — it was a design decision they had made — and if they had any kind of clue they would have known that users would hate having a rootkit on their machines, especially one that provided an obvious hiding place for other malware. As far as I can see, the only new information F-Secure would have disclosed was that F-Secure planned to treat the program as malware.

It's interesting, too, that other makers of anti-malware tools didn't seem to notice the problem until Mark Russinovich's public disclosure. As of mid-September, this malware had been on the market for months and presumably had been installed on hundreds of thousands of computers, but still none of the anti-malware vendors had discovered it. (According to the Business Week article, F-Secure didn't discover the malware itself, but learned of it on Sept. 30 from John Guarino, a computer technician in New York who had discovered it on several clients' computers.) It's not a good

sign that all of the major anti-malware vendors missed it for so long.

Finally, we have to consider the possibility that Sony and First4Internet understood the significance of the rootkit, but simply felt that copy protection trumped users' security. First4Internet probably held that view — otherwise it's hard to explain their design decision to deploy rootkit functionality — and Sony may well have held it too. We know already that entertainment companies want to redesign our computers in the hope (which is ultimately futile) of stopping copying. From there, it's not so large a step to decide that users' security simply must be sacrificed on the altar of copy protection.

What did SonyBMG know, and when did it know it? We'll find out more as the lawsuits proceed.

This entry was posted on Wednesday November 30, 2005 at 6:41 am and is filed under [Security](#), [DRM](#), [Privacy](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

#### **Vulnerability Scanner**

How vulnerable are your networks? Find out with the SAINT Scanner.

#### **Free Vulnerability Scan**

Totally Free Vulnerability scan by Comodo.

[Ads by Goooooogle](#)

[Advertise on this site](#)

## **20 Responses to “Sony, First4 Knew About Rootkit Issue in Advance”**

1. *dr2chase* Says:  
[November 30th, 2005 at 8:40 am](#)

I think “on the altar of copy protection” should be rephrased “to the lucky rabbit’s foot of copy protection”. Lots of ordinary non-piratical users either use Macs, or Linux, or disable autorun with TweakUI. Real live pirates might employ more arcane tricks liking holding down the shift key, optically blocking the data area (tape or marker) or, perish the thought, actually ripping from the audio signal (I’ve got vinyl I’ve converted to MP3; it’s not rocket science, and the results are not bad even from aged records on a garbage-sale turntable).

My theory (“watch what they do, not what they say”) is that this is not about copy protection; it is instead about making computers an unacceptable platform for audio and video. If they cannot control it, then they’ll make it unusable instead. The more interesting question is whose side the anti-spyware and anti-virus companies are on? They’re not normally thought of as an anti-spyware/virus company, but I’ve had pretty good luck with Apple so far.

2. *jordan vance* Says:  
[November 30th, 2005 at 8:49 am](#)

It sounds, or rather looks, to me that Sony had no clue according to that article. It says nothing of SonyBMG being on the first conference call (although my guess is that they had legal beagles who were on that call). If that’s the case, did F-Secure go back to Sony and say that F4I was being harmful? It’ll be interesting to see how this all plays out. F4I won’t come out looking pretty, but I don’t know whether any mud will get smeared on Sony.

3. *The PC Doctor* Says:  
[November 30th, 2005 at 9:25 am](#)

### **Sony knew about the rootkit before the storm!**

BusinessWeek is reporting that Sony BMG knew about the rootkit nearly a month before Mark Russinovich broke the news on Oct 31st.

According to the article, F-Secure informed them on Oct 4th after a PC tech reported the rootkit to them on ...

4. *wouldUbelieve* Says:  
[November 30th, 2005 at 9:52 am](#)

# EXHIBIT 2

# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [SonyBMG DRM Customer Survival Kit](#)  
[Don't Use Sony's Web-based XCP Uninstaller](#) »

## Sony Shipping Spyware from SunnComm, Too

Saturday November 12, 2005 by J. Alex Halderman

Now that virus writers have [started exploiting](#) the rootkit built into Sony-BMG albums that utilize First4Internet's XCP DRM (as I [warned](#) they would last week), Sony has at last [agreed](#) to temporarily stop shipping CDs containing the defective software:

We stand by content protection technology as an important tool to protect our intellectual property rights and those of our artists. Nonetheless, as a precautionary measure, SONY BMG is temporarily suspending the manufacture of CDs containing XCP technology. We also intend to re-examine all aspects of our content protection initiative to be sure that it continues to meet our goals of security and ease of consumer use.

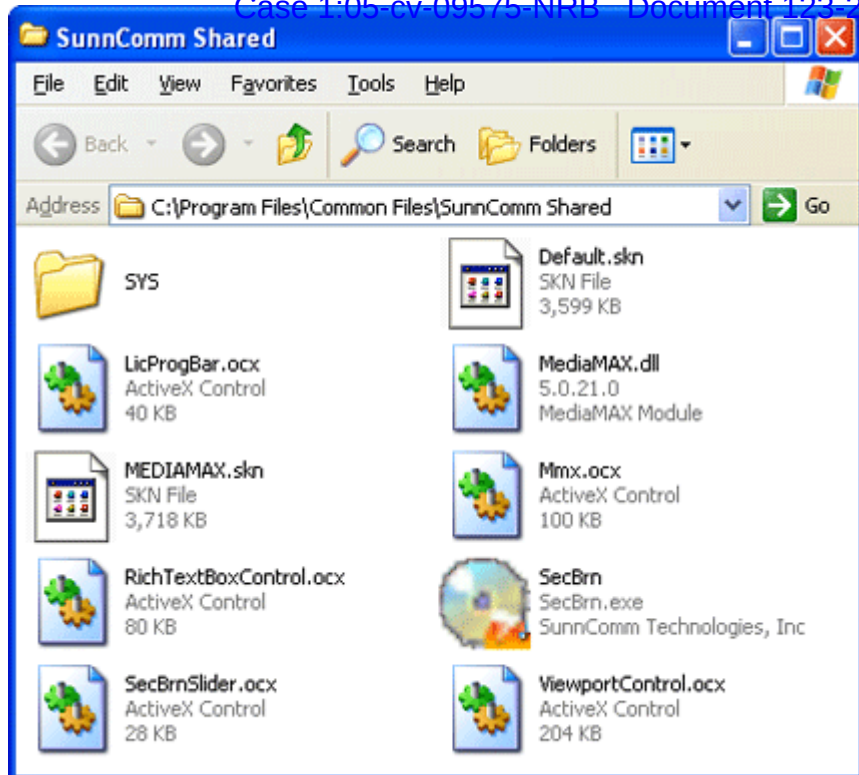
What few people realize is that Sony uses another copy protection program, [SunnComm](#)'s MediaMax, on other discs in their catalog, and that this system presumably is not included in the moratorium. Though MediaMax doesn't resort to concealing itself with a rootkit, it does behave in several ways that are characteristic of spyware.

I originally [wrote about](#) MediaMax back in 2003. It was the first copy restricting technology that installed software in an attempt to block ripping and copying. SunnComm has continued to develop its anti-copying tools, and today MediaMax is distributed on albums from Sony-BMG and several smaller labels. Sony titles that use MediaMax include [Grown and Sexy](#) by Babyface and [Z](#) by My Morning Jacket. These discs aren't hard to spot; the back album covers usually contain a label that includes a sunncomm.com URL.

Like XCP, recent versions of MediaMax engage in spyware-style behavior. They install software without meaningful consent or notification, they include either no means of uninstalling the software or an uninstaller that claims to remove the entire program but doesn't, and they transmit information about user activities to SunnComm despite statements to the contrary in the end user license agreement and on SunnComm's web site. I'll describe each of these problems in detail below.

### **1. MediaMax installs without meaningful consent or notification**

When a MediaMax-protected CD is inserted into a computer running Windows, the Windows Autorun feature launches a program from the CD called PlayDisc.exe. Like most installers, this program displays a license agreement, which you may accept or decline. But *before the agreement appears*, MediaMax installs around a dozen files that consume more than 12 MB on the hard disk. Most are copied to the folder `c:\Program Files\Common Files\SunnComm Shared\`, shown below:



These files remain installed even if you decline the agreement. One of them, a kernel-level driver with the cryptic name “sbcphid”, is both installed and launched. This component is the heart of the copy protection system. When it is running, it attempts to block CD ripping and copying applications from reading the audio tracks on SunnComm-protected discs. ~~MediaMax refrains from making one final change until after you accept the license — it doesn’t set the driver to automatically run again every time Windows starts. Nevertheless, the code keeps running until the computer is restarted and remains on the hard disk indefinitely, even if the agreement is declined.~~ [Update 11/28: In several [common scenarios](#), MediaMax goes a step further and sets the driver to automatically run again every time Windows starts, even if the user has never agreed to the license.]

To see if SunnComm’s driver is present on a Windows XP system, open the start menu and select Run. In the box that pops up, type

```
cmd /k sc query sbcphid
```

and click OK. If the response includes “STATE: 1 STOPPED”, the driver is installed; if it includes “STATE: 4 RUNNING”, the driver is installed and actively restricting access to music. Alternately, you can look for the driver’s file, sbcphid.sys, which will be located in the c:\windows\system32\drivers\ folder if it is installed.

(Newer version of SunnComm’s software can also block copying on Mac systems, as reported by [MacInTouch](#). However, since Mac OS X does not automatically run software from CDs, Mac users will only be affected if they manually launch the installer.)

Is there any meaningful notice before the program is installed? On the contrary, the Sony license agreement (which happens to be identical to the agreement on XCP discs, despite significant differences between XCP and MediaMax) states that the software will not be installed until after you accept the terms:

As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the “SOFTWARE”) onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER until removed or deleted.

Notice too that while the agreement partially describes the protection software, it fails to disclose important details

about what the software does. Yes, the MediaMax driver tries to “protect the audio files embodied on the CD,” but it also attempts to restrict access to *any other* CD that use SunnComm’s technology. You only need to agree to installation on one album for the software to affect your ability to use many other titles.

## 2. MediaMax discs include either no uninstaller or an uninstaller that fails to remove major components of the software

None of the MediaMax albums I’ve seen from Sony-BMG include any option to uninstall the software. However, some titles from other labels do include an uninstall program. For instance, the album [You Just Gotta Love Christmas](#) by Peter Cetera (Viasstar Records) adds MediaMax to the Windows Add/Remove Programs control panel, the standard interface for removing programs. If you elect to remove the software, it displays the following prompt:



Clicking “Yes” does cause parts of MediaMax to be deleted, including nearly all the files in the SunnComm shared folder. However, the protection driver remains installed and active despite the suggestion that “MediaMax and all of its components” would be removed. That means iTunes and other programs still cannot access music for any SunnComm-protected CD.

[**Update:** Apparently SunnComm was providing an uninstaller to users who persistently demanded one, but the uninstaller opened a [severe security hole](#) in users’ systems.]

## 3. MediaMax transmits information about you to SunnComm without notification or consent

Sony and SunnComm seem to go out of their way to suggest that MediaMax doesn’t collect information about you. From the EULA:

[T]he SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise.

SunnComm’s customer care web page is equally explicit:

**Is any personal information collected from my computer while using this CD?:**

No information is ever collected about you or your computer without you consenting.

Yet like XCP, the MediaMax software “phones home” to SunnComm every time you play a protected CD. Using standard network monitoring tools, you can observe MediaMax connecting to the web server `license.sunncomm2.com` and sending the following request headers:

```
POST /perfectplacement/retrieveassets.asp?id=
7F63A4FD-9FBD-486B-B473-D18CC92D05C0 HTTP/1.1
Accept: */*
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: license.sunncomm2.com
Content-Length: 39
Connection: Keep-Alive
Cache-Control: no-cache
```

This shows that MediaMax opens a web page from a SunnComm server and sends a 32-character identifier



(highlighted)—apparently a unique code that tells SunnComm what album you're listening to. The request also contains standard HTTP headers from which the company can learn what operating system you are running (in the above example, NT 5.1, a.k.a. Windows XP) and what version of Internet Explorer you use (here, IE 6).

SunnComm also gets to observe your computer's IP address, which is transmitted to every Internet server you connect to. You are assigned an IP address by your Internet service provider or system administrator. Many users are issued frequently changing "dynamic" IP addresses that make it difficult to track them individually, but others have fixed, "static" addresses. If you have a fixed address, SunnComm can piece together the messages from your computer to find out all the protected discs you listen to and how often you play them. In some cases, such as if you are a Princeton student, knowing the address is enough to let SunnComm track down your name, address, and phone number.

So why does MediaMax contact a SunnComm server in the first place? The server's response to the above request isn't very informative:

Microsoft VBScript runtime

error '800a000d'

Type mismatch: 'ubound'

/perfectplacement/retrieveassets.asp, line 26

Apparently a bug in the server software prevents it from returning any useful information. However, the name "Perfect Placement" in the URL provides a valuable clue about the server's purpose. A SunnComm web page [describes](#) "Perfect Placement" as a MediaMax feature that allows record labels to "[g]enerate revenue or added value through the placement of 3rd party dynamic, interactive ads that can be changed at any time by the content owner." Presumably the broken site is supposed to return a list of ads to display based on the disc ID.

Just because the server software is buggy doesn't mean it isn't collecting data. If SunnComm's web site is configured like most web servers, it logs the information described above for every request. We can't know for certain what, if anything, SunnComm does with the data, but that's why transmitting it at all raises privacy concerns.

...

To summarize, MediaMax software:

- Is installed onto the computer without meaningful notification or consent, and remains installed even if the license agreement is declined;
- Includes either no uninstall mechanism or an uninstaller that fails to completely remove the program like it claims;
- Sends information to SunnComm about the user's activities contrary to SunnComm and Sony statements and without any option to disable the transmissions.

Does MediaMax also create security problems as serious as the Sony rootkit's? Finding out for sure may be difficult, since the license agreement specifically prohibits disassembling the software. However, it certainly causes unnecessary risk. Playing a regular audio CD doesn't require you to install any new software, so it involves minimal danger. Playing First4Internet or SunnComm discs means not only installing new software but trusting that software with full control of your computer. After last week's revelations about the Sony rootkit, such trust does not seem well deserved.

Viewed together, the MediaMax and XCP copy protection schemes reveal a pattern of irresponsible behavior on the parts of Sony and its pals, SunnComm and First4Internet. Hopefully Sony's promised re-examination of its copy protection initiatives will involve a hard look at both technologies.

This entry was posted on Saturday November 12, 2005 at 12:30 am and is filed under [Security](#), [DRM](#), [Privacy](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

# EXHIBIT 3



# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [Immunize Yourself Against Sony's Dangerous Uninstaller Does Sony's Copy Protection Infringe Copyrights?](#) »

## Not Again! Uninstaller for *Other* Sony DRM Also Opens Huge Security Hole

Thursday November 17, 2005 by J. Alex Halderman

I have good news and bad news about Sony's other CD DRM technology, the SunnComm MediaMax system. (For those keeping score at home, Ed and I have written a lot recently about Sony's XCP copy protection technology, but this post is about a separate system that Sony ships on other CDs.)

I [wrote](#) last weekend about SunnComm's spyware-like behavior. Sony CDs protected with their technology automatically install several megabytes of files without any meaningful notice or consent, silently phone home every time you play a protected album, and fail to include any uninstall option.

Here's the good news: As several readers have pointed out, SunnComm will provide a tool to uninstall their software if users pester them enough. Typically this requires at least two rounds of emails with the company's support staff.

Now the bad news: It turns out that the web-based uninstaller SunnComm provides opens up a major security hole very similar to the one created by the web-based uninstaller for Sony's other DRM, XCP, that we [announced](#) a few days ago. I have verified that it is possible for a malicious web site to use the SunnComm hole to take control of PCs where the uninstaller has been used. In fact, the the SunnComm problem is easier to exploit than the XCP uninstaller flaw.

To be clear, the SunnComm security flaw does not apply to the software that ships on CDs, but only to the uninstaller that SunnComm distributes separately for removing the CD software. So if you haven't used the uninstaller, you're not vulnerable to this flaw and you don't need to do anything.

If you visit the SunnComm uninstaller web page, you are prompted to accept a small software component—an ActiveX control called AxWebRemoveCtrl created by SunnComm. This control has a design flaw that allows any web site to cause it to download and execute code from an arbitrary URL. If you've used the SunnComm uninstaller, the vulnerable AxWebRemoveCtrl component is still on your computer, and if you later visit an evil web site, the site can use the flawed control to silently download, install, and run any software code it likes on your computer. The evil site could use this ability to cause severe damage, such as adding your PC to a botnet or erasing your hard disk.

You can tell whether the vulnerable control is installed on your computer by using our [AxWebRemoveCtrl detector](#).

We have created a tool that will disable the control and/or block it from being installed. To apply our tool, download [this file](#) to a temporary location, then double click on the file's icon in Windows. (Windows may ask you to confirm that you wish to add the information in the file to the system registry—choose "Yes.") After the tool has been applied, you may delete the file you downloaded. The tool will take effect as soon as you close and restart Internet Explorer. We recommend that anyone who has used the SunnComm uninstaller run our tool as soon as possible.

Unfortunately, if you use our tool to block the control, you won't be able to use SunnComm's current uninstaller to remove their software. It's up to them to replace the flawed uninstaller with a safe one as soon as possible, and to contact those who have already used the vulnerable uninstaller with instructions for closing the hole.

UPDATE (Nov. 18): We are currently helping SunnComm test a new version of the uninstaller.

This entry was posted on Thursday November 17, 2005 at 1:46 pm and is filed under [Security](#), [DRM](#), [Privacy](#), [CD Copy Protection](#). You can

# EXHIBIT 4

## Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [Does Sony's Copy Protection Infringe Copyrights?](#)  
[What Does MediaMax Accomplish?](#) »

## More Suits Filed; MediaMax Insecurity Remains

Tuesday November 22, 2005 by Ed Felten

Yesterday two lawsuits were filed against Sony, by the [Texas Attorney General](#) and the [EFF](#). The Texas suit claims that Sony's XCP technology violates the state's spyware law. The EFF suit claims that two Sony technologies, XCP and MediaMax, both violate various state laws.

One interesting aspect of the EFF suit is its emphasis on MediaMax. Most of the other lawsuits have focused on Sony's other copy protection technology, XCP. The EFF suit does talk about XCP, but only after getting through with MediaMax. Emphasizing MediaMax seems like a smart move — while Sony has issued an apology of sorts for XCP and has recalled XCP discs, the company is still stonewalling on MediaMax, even though MediaMax raises issues almost as serious as XCP.

As Alex [wrote](#) last week, MediaMax is spyware: it installs software without notice or consent; it phones home and sends back information without notice or consent; and it either doesn't offer an uninstaller or makes the uninstaller difficult to get and use. MediaMax lacks the rootkit-like feature of XCP, but otherwise MediaMax shares all of the problems of XCP, including serious security problems with the uninstaller (mitigated by the difficulty of getting the uninstaller; see above).

But even if all these problems are fixed, the MediaMax software will still erode security, for reasons stemming from the basic design of the software.

For example, MediaMax requires administrator privileges in order to listen to a CD. You read that right: if you want to listen to a MediaMax CD, you must be logged in with enough privileges to manipulate any part of the system. The best practice is to log in to an ordinary (non-administrator) account, except when you need to do system maintenance. But with MediaMax, you must log in to a privileged account or you can't listen to your CD. This is unnecessary and dangerous.

Some of the security risk of MediaMax comes from the fact that users are locked into the MediaMax music player application. The player app evades the measures designed to block access to the music; and of course the app can't play non-MediaMax discs, so the user will have to use multiple music players. Having this extra code on the system, and having to run it, increases security risk. (And don't tell me that music players don't have security bugs — we saw two serious security bugs in Sony music software last week.) Worse yet, if a security problem crops up in the MediaMax player app, the user can't just switch to another player app. More code, plus less choice, equals more security risk.

Worse yet, one component of MediaMax, a system service called sbcphid, is loaded into memory and ready to run at all times, even when there is no disc in the CD drive and no music is being played. And it runs as a kernel process, meaning that it has access to all aspects of the system. This is another component that can only add to security risk; and again the user has no choice.

It's important to recognize that these problems are caused not by any flaws in SunnComm and Sony's execution of their copy protection plan, but from the nature of the plan itself. If you want to try to stop music copying on a PC, you're going to have to resort to these kinds of methods. You're going to have to force users to use extra software that they don't want. You're going to have to invoke administrator privileges more often. You're going to have to keep more software loaded and running. You're going to have to erode users' ability to monitor, control, and secure their systems. Once you set off down the road of copy protection, this is where you're going to end up.

This entry was posted on Tuesday November 22, 2005 at 3:51 am and is filed under [Security](#), [DRM](#), [Privacy](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

# EXHIBIT 5

# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

« [DRM, Incompatibility, and Market Power: A Visit to the Sausage Factory](#)  
[Not Just Another Buggy Program](#) »

## MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug

Wednesday December 7, 2005 by Ed Felten

[iSEC](#), [EFF](#), and [SonyBMG](#) issued a joint [press release](#) yesterday, announcing yet another serious security bug in the SunnComm MediaMax copy protection software that ships on many SonyBMG compact discs. (SonyBMG has recalled CDs that use another copy protection system, XCP, but they have not yet recalled discs containing MediaMax.)

As we've written before, the first time you insert a MediaMax-bearing CD into your Windows computer (assuming you have Windows autorun enabled, as most people do), MediaMax installs some software on your computer. Once this initial software is on your computer, you are vulnerable to the new attack. The gist of the problem is that MediaMax installs itself in a directory that anyone is allowed to modify, even users who otherwise run with heavily restricted security permissions. Any program that comes along can modify your MediaMax files, booby-trapping the files by inserting hostile software that will be run automatically the next time you insert a MediaMax-bearing CD into your computer. And because MediaMax is run with full administrator privileges, the hostile program gets to run with full privileges, allowing it to inflict any mischief it likes on your PC.

Alex Halderman has discovered that the problem is worse than the press release indicates:

- You are vulnerable **even if you decline the MediaMax license agreement**. Simply inserting a MediaMax-bearing CD into your PC paves the way for an attacker to come along and set a booby-trap. The trap will be sprung the next time you insert such a disc.
- SonyBMG has released a patch that purports to fix the problem. However, our tests show that **the patch is insecure**. It turns out that there is a way an adversary can booby-trap the MediaMax files so that hostile software is run automatically *when you install and run the MediaMax patch*.
- **The previously released MediaMax uninstaller is also insecure** in the same way, allowing an adversary to booby-trap files so that hostile software is run automatically when you try to use the uninstaller.

(These attacks are similar to the exploit described in [iSEC's report](#), but they involve a different modification to the MediaMax files.)

Because of these problems, we recommend for now that if you have a Windows PC, you (1) do not use the MediaMax patch, (2) do not use the previously released MediaMax uninstaller, and (3) do not insert a MediaMax-bearing CD into your PC.

We have notified SonyBMG and MediaMax about these problems. We assume they will develop a new uninstaller that safely rids users' computers of the MediaMax software once and for all.

The consequences of this problem are just as bad as those of the XCP rootkit whose discovery by Mark Russinovich started SonyBMG's woes. This problem, like the rootkit, allows any program on the system to launch a serious security attack that would normally be available only to fully trusted programs.

According to the press release, SonyBMG intends to use MediaMax's banner ad display feature to warn users about these vulnerabilities. While this is a positive step, it will fail to reach users who have rejected the MediaMax license agreement. This group is at particularly high risk, since they are probably unaware that the software is installed on their computers.

Worst of all, it is impossible to patch the millions of MediaMax-bearing CDs that are already out there. Every disc sitting on somebody's shelf, or in a record-store bin, is just waiting to install the vulnerable software on the next PC it is inserted into. The only sure way to address this risk is take the discs out of circulation.

The time has come for SonyBMG to recall all MediaMax CDs.

UPDATE (Dec. 9): Sony and MediaMax have issued a new patch. According to our limited testing, this patch does not suffer from the security problem described above. They have also issued a new uninstaller, which we are still testing. We'll update this entry again when we have more results on the uninstaller.

This entry was posted on Wednesday December 7, 2005 at 10:33 am and is filed under [Security](#), [DRM](#), [Privacy](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

#### **Ubeatable Copy Protection**

Alan Technology Technology for Software & Hardware

[Ads by Goooooogle](#)

#### **Digital Video Stabilizer**

Removes copy protection from videotapes. Low price.

[Advertise on this site](#)

## **66 Responses to “MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug”**

1. [Avery J. Parker - Web site hosting and computer service](#) Says:  
[December 7th, 2005 at 11:01 am](#)

[...] Once more in the continuing story.... According to freedom-to-tinker, the “fix” released today for the SunnComm/Mediamax DRM software (the “other” DRM software on sony/bmg discs). Is fatally flawed. The problem the software initially poses is much worse than the company lets on in their release and their advise is.... 1) don't play a mediamax protected disc in your pc. 2)don't use the fix, 3) don't use the old uninstaller. [...]

2. [Eddie hates copy protection](#) Says:  
[December 7th, 2005 at 11:29 am](#)

I'll have to hand it to you Eddie and Alex, you certainly have a penchant to deride Mediamax and an obvious distaste for any kind of audio copy protection in the market place. What are your feelings on game, software and DVD copy protection? Do you feel it is your right to copy those as well?

3. [JayCee](#) Says:  
[December 7th, 2005 at 11:51 am](#)

The list of cd's that MediaMax is oddly only on the “BMG” side of the company's releases- I think it's something like RCA and Jive Records. Any info online from those labels? (example: rcarecords.com)

I noticed that the labels formerly only under Sony have big fat links to XCP info on their sites (like columbiarecords.com)...

4. [AB](#) Says:  
[December 7th, 2005 at 11:52 am](#)

Here's the reply I received from their tech support when I said their ActiveX utility was problematic. If you reboot, does it remove the threat?

“Unfortunately, this is the only means by which to uninstall MediaMax. However, as previously noted, the Active X control installed is removed upon your next reboot. It will list all files left on the system as they are system files only shared by MediaMax. There is no security risk involved with this removal process. Due to recent media involving problems with other copy protection softwares, our utility has been tested extensively, both interneally and externally, and there is zero security risk. If you wish to uninstall MediaMax from your system, you must use this utility.”

# EXHIBIT 6

# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug](#)  
[CD Copy Protection: The Road to Spyware](#) »

## Not Just Another Buggy Program

Thursday December 8, 2005 by Ed Felten

Was anybody surprised at Tuesday's announcement that the MediaMax copy protection software on Sony CDs had a serious security flaw? I sure wasn't. The folks at iSEC Partners were clever to find the flaw, and the details they uncovered were interesting, but it was pretty predictable that a problem like this would turn up.

Security is all about risk management. If you're careful to avoid unnecessary risks, to manage the risks you must accept, and to have a recovery plan for when things go wrong, you can keep your security under control. If you plunge ahead, heedless of the risks, you'll be sorry.

If you're a parent, you'll surely remember the time your kid left an overfull glass of juice on the corner of a table and, after the inevitable spill, said, "It was an accident. It's not my fault." And so the kid had to learn why we don't set glasses at the very edges of tables, or balance paintbrushes on the top of the easel, or leave roller skates on the stairs. The accident won't happen every time, or even most of the time, but it will happen eventually.

If you're a software vendor, your software creates risks for its users, and you have a responsibility to your customers to help them manage those risks. You should help your customers make informed choices about when and how to use your software, and you should design your software to avoid exposing customers to unnecessary risks. Your customers expect this from you, and they'll hesitate to buy your product if they think you're leaving the cyberjuice on the corner of the table.

The design of the MediaMax/Sony software is a case study in risk creation. I [wrote](#) about these risks two weeks ago:

But even if all [the software's spyware] problems are fixed, the MediaMax software will still erode security, for reasons stemming from the basic design of the software.

For example, MediaMax requires administrator privileges in order to listen to a CD. You read that right: if you want to listen to a MediaMax CD, you must be logged in with enough privileges to manipulate any part of the system. The best practice is to log in to an ordinary (non-administrator) account, except when you need to do system maintenance. But with MediaMax, you must log in to a privileged account or you can't listen to your CD. This is unnecessary and dangerous.

Some of the security risk of MediaMax comes from the fact that users are locked into the MediaMax music player application. The player app evades the measures designed to block access to the music; and of course the app can't play non-MediaMax discs, so the user will have to use multiple music players. Having this extra code on the system, and having to run it, increases security risk. (And don't tell me that music players don't have security bugs — we saw two serious security bugs in Sony music software last week.) Worse yet, if a security problem crops up in the MediaMax player app, the user can't just switch to another player app. More code, plus less choice, equals more security risk.

Sure enough, these risks enable the new attack, which exploits the presence of extra code on the system, and the fact that that code runs with full Administrator privileges.

The biggest risk of all, though, is that the software can install itself without the knowledge or consent of the user. When you decide to install a program on your computer, you take a security risk. But you take that risk knowingly, because



you have decided the benefit provided by that program outweighs the risk. If you change your mind about that tradeoff, you can always uninstall the program.

But if you decline the MediaMax licence agreement, and the software secretly installs itself anyway, you will face risks that you didn't choose. You won't even know that you're at risk. All of this, simply because you tried to listen to a compact disc.

Experience teaches that where there is one bug, there are probably others. That's doubly true where the basic design of the product is risky. I'd be surprised if there aren't more security bugs lurking in MediaMax.

Sony is still shipping CDs containing this dangerous software.

This entry was posted on Thursday December 8, 2005 at 8:01 am and is filed under [Security](#), [DRM](#), [Privacy](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

#### **Ubeatable Copy Protection**

Alan Technology Technology for Software & Hardware

[Ads by Goooooogle](#)

#### **MySpace Turned Inside-Out**

Meet others online, share your pictures, and blog for free.

[Advertise on this site](#)

## **49 Responses to "Not Just Another Buggy Program"**

1. [Greg](#) Says:  
[December 8th, 2005 at 8:37 am](#)

I've been an avid follower of your posts and dissection of Sony's programming and consumer failure. For 36 days I've been battling with Sony Customer Service and their ContentProtectionHelp (ContentProtectionHelp@info.sel.sony.com) department working on this CD issue, with more than 14 e-mails back and forth and more than 3 hours logged on the phone.

I want three things: -a "clean" version of the CD I purchased, -my computer 100 percent back to normal, -an apology and compensation for my trouble.

To date, I haven't received any of these three, and Sony Customer Service has not offered any acknowledgement of error on their part. They appear to have lost my CD that I mailed back to them and blame me for that. They appear to have released a standalone uninstaller, but thanks to your insightful monitoring of their constant failure to release bug-free software, I do not trust them to run it. They have only offered me the option to wait until after 2006 when they will have a better handle on things.

Considering I purchased/installed the CD/malware on Nov. 1, this is unacceptable to me as an unwitting consumer. But of course, they don't care. I'm just another dumb, complaining customer.

2. [Anonymous](#) Says:  
[December 8th, 2005 at 8:43 am](#)

Ed, in your experience, what percent of software programs are completely bug free?

3. [Ed Felten](#) Says:  
[December 8th, 2005 at 8:51 am](#)

Anonymous,

All programs have bugs. The number and severity of those bugs, and the level of harm they inflict on users, varies greatly, depending on how responsible the vendor is about managing risks. Careless vendors make bug risks much worse.

# EXHIBIT 7

# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [RIAA Critics, and their Critics, Debate Lawsuits](#)  
[SonyBMG DRM Customer Survival Kit](#) »

## SonyBMG “Protection” is Spyware

Thursday November 10, 2005 by Ed Felten

Mark Russinovich has yet another great [post](#) on the now-notorious SonyBMG/First4Internet CD “copy protection” software. His conclusion: “Without exaggeration I can say that I’ve analyzed virulent forms of spyware/adware that provide more straightforward means of uninstall.”

Here’s how the uninstall process works:

- The user somehow finds the obscure web page from which he can request the uninstaller.
- The user fills out and submits a form requesting the uninstaller. The form requests information that is not necessary to perform the uninstallation.
- The vendor sends the user an email asking them to install a patch, and then to visit another page if he still wants to uninstall the software.
- The user is directed to install and run yet more software — an ActiveX control — on his computer.
- The user has to fill out and submit yet another form, which asks unnecessarily for still more information.
- The vendor sends the user an email containing a cryptic web link.
- The user clicks on that web link. This will perform the uninstall, but only if the user is running on the same computer on which he performed the previous steps, and only if it is used within one week.

None of these steps is necessary. It would be perfectly feasible to provide for download a simple uninstaller that works on any computer that can run the original software. Indeed, it would have been easier for the vendor to do this.

In all the discussion of the SonyBMG software, I’ve been avoiding the S-word. But now it’s clear that this software crosses the line. It’s spyware.

Let’s review the evidence:

- The software comes with a EULA which, at the very least, misleads users about what the software does.
- The software interferes with the efforts of ordinary users and programs, including virus checkers and other security software, to identify it.
- Without telling the user or obtaining consent, the software sends information to the vendor about the user’s activities.
- No uninstaller is provided with the software, or even on the vendor’s website, despite indications to the contrary in the EULA.
- The vendor has an uninstaller but refuses to make it available except to individual users who jump through a long series of hoops.
- The vendor makes misleading statements to the press about the software.

This is the kind of behavior we’ve come to expect from spyware vendors. Experience teaches that it’s typical of small DRM companies too. But why isn’t SonyBMG backing away from this? Doesn’t SonyBMG aspire to at least a modest level of corporate citizenship?

There are three possibilities. Maybe SonyBMG is so out of touch that they don’t even realize they are in the wrong. Or maybe SonyBMG realizes its mistake but has decided to stonewall in the hope that the press and the public will lose interest before the company has to admit error. Or maybe SonyBMG realizes that its customers have good reason to be

angry, but the company thinks it is strategically necessary to defend its practices anyway. The last possibility is the most interesting; I may write about it tomorrow.

Outside the SonyBMG executive suite, a consensus has developed that this software is dangerous, and forces are mobilizing against it. Virus researchers are [analyzing](#) malware now in circulation that exploits the software's rootkit functionality. Class-action lawsuits have been filed in California and New York, and a government investigation seems likely in Italy. Computer Associates has [labeled](#) the software as spyware, and modified its PestPatrol spyware detector to look for the software. Organizations such as Rutgers University are even warning their people not to play SonyBMG CDs in their computers.

This entry was posted on Thursday November 10, 2005 at 8:25 am and is filed under [Security](#), [DRM](#), [Privacy](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

#### **Free Ad & Spyware Remover**

Remove Adware & Spyware, Free. Full version only from Privacy Crusader.

[Ads by Goooooogle](#)

#### **Ad-ware - (Free Download)**

2006 Highly-Rated Adware Remover. Kill Popups & Viruses in 2 Minutes!

[Advertise on this site](#)

## 16 Responses to “SonyBMG “Protection” is Spyware”

### 1. *Grant Gould* Says:

[November 10th, 2005 at 9:03 am](#)

As the IT person at a small company (in the streaming music business, no less!), I have banned Sony CDs from any office machine whose Autorun has not been disabled.

I agree that Sony has probably made a strategic decision that this sort of invasive software is what they need in order to fight the DRM war. Their multistage uninstallation process reminds me too much of the elaborate hoops set up for users who play too many out-of-region DVDs — it has the look of an intentional “speedbump” set up to prevent naive users from too easily or causally getting what they want.

### 2. *Mike W* Says:

[November 10th, 2005 at 9:12 am](#)

I'm kind of curious about the implications of web sites offering instructions (disable autorun, hold down shift key, instructions for removal....) for disabling or working around the Sony protections. I thought the DMCA had strict provisions against trafficking in tools and procedures for circumventing a protection device.

Just one of those things that make me go, “hmmmm....”

### 3. *Brian Srivastava* Says:

[November 10th, 2005 at 11:16 am](#)

And now it would seem, not only is the rootkit spyware, but it makes installing trojans that much easier!

[http://www.theregister.co.uk/2005/11/10/sony\\_drm\\_trojan/](http://www.theregister.co.uk/2005/11/10/sony_drm_trojan/)

For once in my life I'm thinking that litigious society the people in the US have to live with my actually have its uses.

### 4. *Todd Jonz* Says:

[November 10th, 2005 at 11:51 am](#)

We should not allow our collective anger at Sony BMG's stonewalling to prevent us from appreciating its humorous aspects, such as Sony Global Digital president Thomas Hesse's statement, “Most people, I think, don't even know what a rootkit is, so why should they care about it?” My immediate thought was, “Most people don't know what radon is, so why should they care if it's accumulating in their basements?”

# EXHIBIT 8

# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [CD DRM Makes Computers Less Secure](#)  
[SonyBMG and First4Internet Release Mysterious Software Update](#) »

## CD-DRM Rootkit: Repairing the Damage

Wednesday November 2, 2005 by Ed Felten

SonyBMG and First4Internet are in the doghouse now, having been caught installing [rootkit-like software](#) on the computers of SonyBMG music customers, thereby exposing the customers to security risk. The question now is whether the companies will face up to their mistake and try to remedy it.

First4Internet seems to be trying to dodge the issue. For example, here's part of a news.com [story](#) by John Borland:

The creator of the copy-protection software, a British company called First 4 Internet, said the cloaking mechanism was not a risk, and that its team worked closely with big antivirus companies such as Symantec to ensure that was the case. The cloaking function was aimed at making it difficult, though not impossible, to hack the content protection in ways that have been simple in similar products, the company said.

In any case, First 4 has moved away from the techniques used on the Van Zant album to new ways of cloaking files on a hard drive, said Mathew Gilliat-Smith, the company's CEO.

"I think this is slightly old news," Gilliat-Smith said. "For the eight months that these CDs have been out, we haven't had any comments about malware (malicious software) at all."

The claim that the software is not a risk is simply false, as Alex [explained](#) yesterday. And if the company is indeed working on new ways to hide the contents of your computer from you, that just shows that they haven't learned their lesson. The problem is not that they used a particular rootkit method. The problem is that they used rootkit methods at all. Switching to a new rootkit method will, if anything, make the problem worse.

The claim that there haven't been any complaints about the software is also false. The reviews on Amazon have plenty of complaints, and there was a [discussion](#) of these problems at CastleCops. And, of course, Mark Russinovich has complained.

The claim that this is old news is just bizarre. First4Internet is offering this system to record companies — today. SonyBMG is selling CDs containing this software — today. And this software is sitting on many users' computers with no uninstaller — today.

If the First4Internet wants to stop spinning and address the problem, and if SonyBMG wants to start recovering consumer trust, I would suggest the following steps.

- (1) Admit that there is a problem. The companies can admit that the software uses rootkit-like methods and may expose some consumers to increased security risk.
- (2) Modify product packaging, company websites, and EULA language to disclose what the software actually does. Thus far there hasn't been adequate notification. For example, the current EULA says this:

As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the "SOFTWARE") onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER

until removed or deleted. However, the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise.

Clearly a rootkit neither protects the audio files nor facilitates use of the content. This is not the only misleading aspect of the description. For example, this does not convey to users that they will be unable to make lawful uses of the music such as downloading it to an iPod, or that there is no way to uninstall the software (indeed, it strongly implies the opposite), or that attempting to remove the software may make the computer's CD drive inaccessible.

(3) Release a patch or uninstaller that lets any consumer easily remove or disable the rootkit-like functions of the software. Having caused security problems for their users, the least the companies can do is to help users protect themselves.

(4) Make clear that the companies support, and give permission for, research into the security implications of their products. Saying "trust us" won't cut it anymore. Having betrayed that trust once, the companies should publicly welcome the Mark Russinoviches of the world to keep studying their software and publishing what they find. If you act like you have something to hide — and you have had something to hide in the past — the public will be smart enough to conclude that you're probably still hiding something. This is especially true if you announce that you are trying to find new ways to do the thing that you were just caught doing!

Finally, let me just point out two things. First, we don't know yet whether the First4Internet/SonyBMG software causes even more security or privacy problems for users. Given what we've seen so far, I wouldn't be at all surprised if there are more problems lurking.

Second, this general issue applies not only to F4I and SonyBMG's technology. Any attempt to copy-protect CDs will face similar problems, because this kind of copy-protection software has a lot in common with standard malware. Most notably, both types of software try to maintain themselves on a user's computer against the user's will — something that cannot be done without eroding the user's control over the computer and thereby inhibiting security.

If you're using a recent version of Windows, you can protect yourself against this type of software, and some other security risks, by [disabling autorun](#).

This entry was posted on Wednesday November 2, 2005 at 7:58 am and is filed under [Security](#), [DRM](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

#### **Ubeatable Copy Protection**

Alan Technology Technology for Software & Hardware

Ads by Goooooogle

#### **MySpace Turned Inside-Out**

Meet others online, share your pictures, and blog for free.

[Advertise on this site](#)

## **37 Responses to "CD-DRM Rootkit: Repairing the Damage"**

1. *matt* Says:

[November 2nd, 2005 at 9:45 am](#)

or maybe someone in congress could just pass the Digital Media Consumers' Rights Act (<http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.107:>) so that SonyBMG would have to put a big label on the disk that says "this won't work for you!".

2. *Mat Hall* Says:

[November 2nd, 2005 at 10:38 am](#)

*Most notably, both types of software try to maintain themselves on a user's computer against the user's will — something that cannot be done without eroding the user's control over the computer and thereby inhibiting security.*

This is a pretty good summary of the UK Computer Misuse Act, and although IANAL I'd be fairly confident that they could be successfully prosecuted. Any enterprising lawyers out there want to have a go?